CCFA-200 Q&As

CrowdStrike Certified Falcon Administrator

Pass CrowdStrike CCFA-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ccfa-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CrowdStrike Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

One of your development teams is working on code for a new enterprise application but Falcon continually flags the execution as a detection during testing. All development work is required to be stored on a file share in a folder called "devcode."

What setting can you use to reduce false positives on this file path?

A. USB Device Policy

B. Firewall Rule Group

C. Containment Policy

D. Machine Learning Exclusions

Correct Answer: C

QUESTION 2

You have been provided with a list of 100 hashes that are not malicious but your company has deemed to be inappropriate for work computers. They have asked you to ensure that they are not allowed to run in your environment. You have

chosen to use Falcon to do this.

Which is the best way to accomplish this?

A. Using the Support Portal, create a support ticket and include the list of binary hashes, asking support to create an "Execution Prevention" rule to prevent these processes from running

B. Using Custom Alerts in the Investigate App, create a new alert using the template "Process Execution" and within that rule, select the option to "Block Execution"

C. Using IOC Management, gather the list of SHA256 or MD5 hashes for each binary and then upload them. Set all hashes to "Block" and ensure that the prevention policy these computers are using includes the option for "Custom Blocking" under Execution Blocking.

D. Using the API, gather the list of SHA256 or MD5 hashes for each binary and then upload them, setting them all to "Never Allow"

Correct Answer: C

QUESTION 3

When would the No Action option be assigned to a hash in IOC Management?

A. When you want to save the indicator for later action, but do not want to block or allow it at this time

B. Add the indicator to your allowlist and do not detect it

C. There is no such option as No Action available in the Falcon console

D. Add the indicator to your blocklist and show it as a detection

Correct Answer: A

QUESTION 4

If a user wanted to install an older version of the Falcon sensor, how would they find the older installer file?

A. Older versions of the sensor are not available for download

B. By emailing CrowdStrike support at support@crowdstrike.com

C. By installing the current sensor and clicking the "downgrade" button during the install

D. By clicking on "Older versions" links under the Host setup and management > Deploy > Sensor downloads

Correct Answer: D

QUESTION 5

What can the Quarantine Manager role do?

A. Manage and change prevention settings

B. Manage quarantined files to release and download

C. Manage detection settings

D. Manage roles and users

Correct Answer: B

CCFA-200 VCE Dumps CCFA-200 Practice Test CCFA-200 Braindumps